AF$ / IFW

PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re application of	Docket No: A7254 / ST9-98-094
Henry M. GLADNEY	
Appln. No.: 09/465,514	Group Art Unit: 2135
Confirmation No.: 8969	Examiner: Leynna A. HA
Filed: December 16, 1999	

For: DISTRIBUTED DATA STRUCTURES FOR AUTHORIZATION AND ACCESS CONTROL FOR COMPUTING RESOURCES

SUBMISSION OF APPEAL BRIEF

MAIL STOP APPEAL BRIEF - PATENTS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Submitted herewith please find an Appeal Brief. A check for the statutory fee of $500.00 is attached. The USPTO is directed and authorized to charge all required fees, except for the Issue Fee and the Publication Fee, to Deposit Account No. 19-4880. Please also credit any overpayments to said Deposit Account. A duplicate copy of this paper is attached.

Respectfully submitted,

Timothy P. Cremen
Registration No. 50,855

SUGHRUE MION, PLLC
Telephone: (202) 293-7060
Facsimile: (202) 293-7860

WASHINGTON OFFICE
23373
CUSTOMER NUMBER

Date: September 20, 2005

PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re application of	Docket No: A7254 / ST-9-98-094
Henry M. GLADNEY	
Appln. No.: 09/465,514	Group Art Unit: 2135
Confirmation No.: 8969	Examiner: Leynna A. HA
Filed: December 16, 1999	

For: DISTRIBUTED DATA STRUCTURES FOR AUTHORIZATION AND ACCESS CONTROL FOR COMPUTING RESOURCES

APPEAL BRIEF UNDER 37 C.F.R. § 41.37

MAIL STOP APPEAL BRIEF - PATENTS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In accordance with the provisions of 37 C.F.R. § 41.37, Appellant submits the following:

Table of Contents

I. REAL PARTY IN INTEREST

The real party in interest is INTERNATIONAL BUSINESS MACHINES CORPORATION by virtue of an assignment executed by Henry M. Gladney (hereinafter "Appellant") on November 17, 1999.

II. RELATED APPEALS AND INTERFERENCES

To the best of the knowledge and belief of the Appellant, the Assignee and the undersigned, there are no other appeals or interferences before the Board of Appeals and Interferences ("the Board") that will directly affect, or be affected by, the Board's decision in the present Appeal.

III. STATUS OF CLAIMS

Claims 1-42 are all the claims pending in the Application.

Claims 1-42 stand rejected under 35 U.S.C. § 102(e) as being anticipated by *Garg et al.* (US 6,625,603 B1; hereinafter "*Garg*").

IV. STATUS OF AMENDMENTS

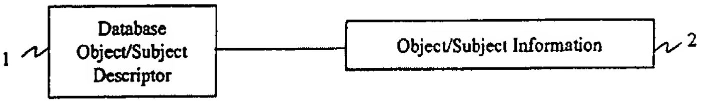
A *Response Under 37 C.F.R. § 1.116* was filed on June 20, 2005, in response to the Final *Office Action* dated April 20, 2005. No changes were made to the claim set by way of the June 20, 2005 *Response*, and no other amendment or response was filed subsequent to the April 20, 2005 Final *Office Action*.

V. SUMMARY OF THE CLAIMED SUBJECT MATTER

To explain the invention for the Board's convenience, Appellants will first describe the relevant art (pp. 1-3 of the Specification), and then the exemplary embodiments of the invention (pp. 7-14 of the Specification). Portions of the claims that correspond to the features shown in the exemplary embodiments are also referenced during this discussion (portions of independent claims 1, 6, 10, 17, 22, 24, 27, 30, 34 and 36 are provided in block quotes for easy identification). This discussion of the exemplary embodiments and the pending claims is provided for explanatory purposes only, and is not intended to limit the scope of the claims.

V(I). Relevant Art

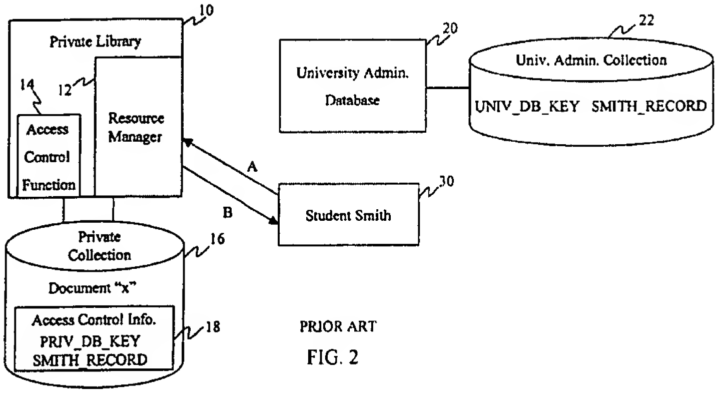
In related art access control systems, the association of user and organization information with each other and with access control information in an administrative domain is too close, effectively limiting an outside user's access to an object. Such arrangements are described further with respect to FIGS. 1 and 2, which are reproduced herein for convenience (p. 1, line 13 - p. 2, line 12).


1
Database Object/Subject Descriptor
Object/Subject Information
2

PRIOR ART

FIG. 1

FIG. 1 illustrates the association between an object or subject information 2 stored in a conventional database and a database descriptor 1 for that object or subject. The descriptor 1 can be used as a key to locate the object or subject information in the database. In such a use, the descriptor 1 is unique within the administrative domain of the database, but is not necessarily unique outside that administrative domain. This non-uniqueness presents a problem when a user outside the administrative domain needs to access an object that is protected, because a fundamental requirement of an access control service is to identify the requested protected object and the user unambiguously (p. 2, lines 13-27).



PRIOR ART
FIG. 2

FIG. 2 illustrates this problem in more detail. In this example (where a library allows university student access to its documents), a university administrative database 20 contains information about Student Smith (*i.e.* SMITH_RECORD), associated with a descriptor (*i.e.*, UNIV_DB_KEY), in collection 22, <u>and</u> a separate private library 10 (which is in an administrative domain separate from university administrative database 20) also contains information about Student Smith (*i.e.*, SMITH_RECORD) associated with a descriptor (i.e., PRIV_DB_KEY) in access control 18. UNIV_DB_KEY and PRIV_DB_KEY are unique within their respective domains, but are <u>different</u> from each other (p. 3, lines 16-26).

In operation, Smith sends (via computer 30) request "A" for access to protected document "x" in the private library's collection 12. Access control function 14 processes the request and determines whether Smith has permission to be given access to document "x" by reviewing access control information 18, which defines information about Smith and his privileges. When it is determined whether Smith can be granted access, access control function 11 returns a yes/no response "B" granting or denying Smith the requested access (p. 3, lines 6-15).

However, as noted above, the university's administrative database 20 also contains access control information about Student Smith (*i.e.*, UNIV_DB-KEY SMITH-RECORD in collection 22). Thus, the access control information 18 in library 10 is redundant. It can easily be understood that this redundancy creates problems in this exemplary embodiment, since the turnover of students every year at the university will require much updating of the library's separate access control information 18 (p. 2, lines 1-7).

V(II). Exemplary Embodiments of the Invention

Accordingly, Appellant's invention is directed to the use of Universal Unique Identifiers (UUIDs) as descriptors in a distributed system, so that conventional access control systems may be extended by distributing user or subject descriptions into one or more systems connected remotely from each other (p. 6, lines 1-10).

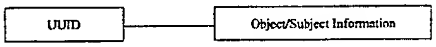


FIG. 3

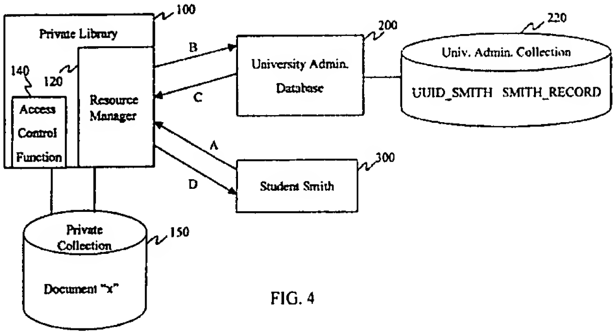


FIG. 4

FIGS. 3 and 4 illustrate a first exemplary embodiment of Appellant's invention. As noted above, FIG. 3 shows that a UUID is utilized to uniquely describe object and/or subject information.

FIG. 4 shows an access control system [1] similar to the university/private library example discussed above. This access control system utilizes a university administration database 200 [2] / administrative collection 220 (*i.e.*, a storage system) having a student record

[1] This supports the recitation of dependent claim 6 and 10 that "the storage system is part of an access control system."

(*i.e.*, SMITH_RECORD - an object) stored therein, each of which are bound to a UUID [3] (*i.e.*, UUID_SMITH - an object identifier that is unique) stored therein. Only this one record describing Student Smith (*i.e.*, UUID_SMITH SMITH_RECORD) is utilized by both the university database 200 and the private library 100 (*i.e.*, both inside and outside of university database 200) (p. 7, line 8 - p. 9, line 4).

The following independent claims are supported by these exemplary features.

Claim 1

1. A storage system comprising:

a first storage area having an object stored therein; and

a second storage area having stored therein an object identifier that identifies the object, wherein the object identifier is unique within and outside of the storage system.

Claim 6

6. A memory comprising:

a first storage area having an object stored therein; and

a second storage area having stored therein an object identifier that identifies the object, wherein the object identifier is unique within and outside of the storage system.

Claim 10

10. A method of storing information in a storage system, comprising:

storing an object in the storage system; and

storing an object identifier in the storage system, wherein the object identifier identifies the object, and the object identifier is unique within and outside of the storage system.

More specifically, the access control system allows Smith (*i.e.*, a requestor) to first send a request "A" for document "x" (i.e., requesting access for a user) specifying at least an identifier for document "x" and the UUID (i.e, UUID_SMITH) for Smith's administrative information (i.e., a subject identifier that identifies the user) held in the university's administrative database 200) [4] to the private library's access control function 140 (i.e., a protecting reference monitor or

[2] This supports the recitation of dependent: (1) claim 3 and 8 that "the first and second storage areas are storage areas within a database;" (2) claim 12 that "the object is stored in a database;" (3) claim 13 that "the object identifier is stored in a database;" and (4) claims 38, 39 and 40 that "the object is a database record describing a user."

[3] This supports the recitation in dependent claims 2, 4, 7, 9, 11, 14 and 15 that "the object identifier is a Universal Unique Identifier (UUID)."

[4] This supports the recitation in dependent claim 19 that "the request further includes a subject descriptor for use in the access control decision."

access control unit). Upon receiving request "A", the access control function 140 resolves the UUID and determines the location of the subject information described by the UUID [5] (in this case the location is the university's administrative database 200). Then, access control function 110 sends a request "B" containing the UUID (*i.e.*, UUID_SMITH) to university database 200 to retrieve portions of the subject information (*i.e.*, SMITH_RECORD) so that the retrieved portions may be used to perform the access control services (p. 9, lines 5-23).

The following independent claims are supported by the above features.

Claim 17

17. (Original) An access control method comprising:

requesting access for a user to a remote resource, wherein the request includes a subject identifier for use in making an access control decision, and wherein the subject identifier is unique within and outside of the remote resource and identifies the user.

Claim 22

22. (Original) A computer-readable medium having computer-executable code stored thereon, comprising:

computer instructions for requesting access for a user to a remote resource, wherein the request includes a subject identifier for use in making an access control decision, and wherein the subject identifier is unique within and outside of the remote resource and identifies the user.

Next, upon receiving request "B" including the subject UUID, the university's administrative database 200 finds the subject information [6] (*i.e.*, SMITH_RECORD) and returns the requested portions of it to the private library in response "C" (*i.e.*, a response including user information). Upon receiving the subject information in response "C", the access control function 140 then determines whether to grant Smith permission to requested document "x", and

[5] Dependent claim 18, 20, 23, 35, 37's recitation that "the subject identifier is a Universal Unique Identifier (UUID)."

[6] This supports the recitation in dependent claims 41 and 42 that "the subject identifier identifies a database record describing the user, and the database record is stored on a local resource physically separate from the remote resource."

returns a yes/no response "D" to Smith.[7] In this (and the following) embodiment, the requests and response messages travel over secure and trusted communications links (p. 9, line 24, p. 10, line 10).[8]

The following independent claims are supported by the above features.

Claim 24

24. (Original) A method of identifying a user requesting access to an object, comprising:

establishing a secure communication path between a reference monitor protecting the object and a resource manager having information describing the user, in response to a request by the user to access the object;

sending a request for user information from the protecting reference monitor to the resource manager, the request including a subject descriptor for the user, wherein the subject identifier is a Universal Unique Identifier (UUID);

receiving, in response to the request, the user information located based on the subject identifier.

Claim 27

27. (Original) An information storage management system, comprising:

a collection of stored objects;

an access control unit for determining if a requestor is authorized to access a protected object stored in the collection;

a resource manager connected to the access control unit and to a communications channel;

wherein the resource manager receives a user's request for access to the protected object, the request including a globally unique identifier for the user requesting the access, and in response to the user's request the resource manager sends over the communications channel to an external storage management system a request for information about the user, the request including the globally unique identifier; and

wherein the resource manager upon receiving a response including user information about the user passes the user information to the access control unit; and based on the user information the access control unit determines whether to grant the

Claim 30

30. (Previously Presented) An information storage management system, comprising:

a collection of stored objects;

an access control unit for determining if a requestor is authorized to access a protected object stored in the collection;

a resource manager connected to the access control unit and to a communications channel;

wherein the resource manager receives a user's request for access to the protected object, the request including a globally unique identifier for the user requesting the access, and in response to the user's request the resource manager resolves the globally unique identifier to a user identifier recognized by an external storage management system; the resource manager sending to the external storage management system a request for information about the user, the request including the resolved user identifier; and

wherein the resource manager upon receiving a response including user information about the user passes the user information to the access

[7] This supports the recitation in dependent claim 25 of "determining, based on the received user information, if the user has permission to access the requested object."

[8] This supports the recitation in dependent claim 21 that "the request is sent over a communications path considered safe by the protecting resource manager and the user."

subject access to the protected object.	control unit; and based on the user information the access control unit determines whether to grant the subject access to the protected object.

Accordingly, the need for the private library to maintain redundant access control information is eliminated, thereby reducing system administration cost and burden. Further, Smith may access the object (*i.e.*, document "x") without burdensome clerical constraints on him (*e.g.*, having to enter a special password conforming to the private library's access control mechanisms) (p. 8, lines 18-23).

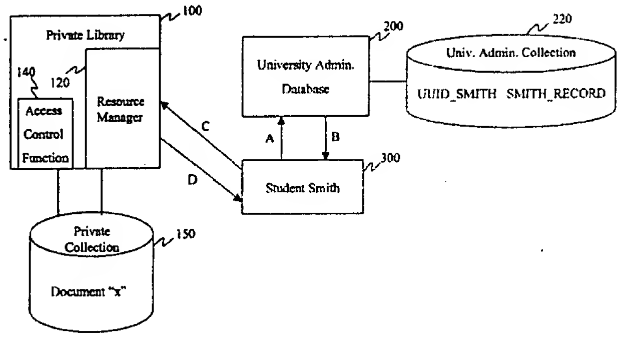


FIG. 5

In a second embodiment of Appellant's invention, shown in FIG. 5 (reproduced to the right for convenience), instead of the access control function 110 resolving the UUID, the user computer 300 gathers from the university's administrative database the subject information required by the access control function 110. More specifically, Smith sends request "A" to the university administrative database 200 with the UUID[2] for the subject information. The database retrieves the information in the same manner as in the first embodiment, but returns it, via response "B", to the user's computer 300. The user's computer 300 then sends to the private library's access control function 110 in request "C" the information retrieved from the university's database, along with a request for document "x" (*i.e.*, a request for access including information about the user). The

[2] This supports the recitation in dependent claims 28 and 31 that "the globally unique identifier is a Universal Unique Identifier (UUID)."

access control function is performed in the same manner as previously described and a yes/no response "D" is returned to the user, thereby granting or denying Smith access to document "x" (p. 10, lines 13-25).

The following independent claims are supported by the above features.

Claim 27

34. (Previously Presented) A method of accessing a protected object, comprising:

sending a globally unique identifier for a user to a name resolving device, and receiving there from information about the user; and

sending to a storage management system containing an object a request for access to the object, the request including the information about the user.

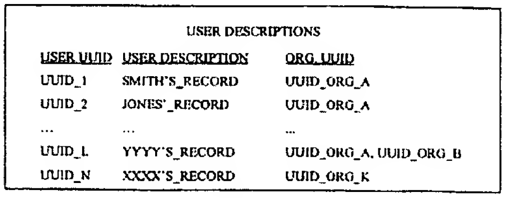
Claim 30

36. (Previously Presented) A computer-readable medium of computer-executable code for accessing a protected object, comprising:

a first set of computer instructions for sending a globally unique identifier for a user to a name resolving device, and receiving there from information about the user; and

a second set of computer instructions for sending to a storage management system containing an object a request for access to the object, the request including the information about the user.

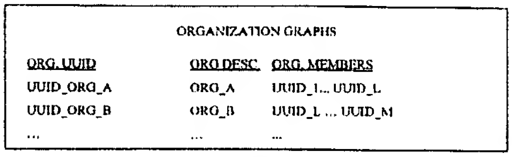
In a third embodiment, as shown in FIGS. 6A-6C (reproduced to the right for convenience), subject information, organization information and object information are bound to UUIDs, which permit even greater distribution of such information.



USER DESCRIPTIONS

USER UUID	USER DESCRIPTION	ORG. UUID
UUID_1	SMITH'S_RECORD	UUID_ORG_A
UUID_2	JONES'_RECORD	UUID_ORG_A
...	...	...
UUID_L	YYYY'S_RECORD	UUID_ORG_A, UUID_ORG_B
UUID_N	XXXX'S_RECORD	UUID_ORG_K

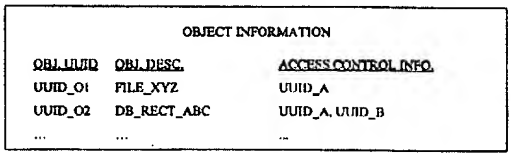
FIG. 6A



ORGANIZATION GRAPHS

ORG. UUID	ORG DESC.	ORG. MEMBERS
UUID_ORG_A	ORG_A	UUID_1... UUID_L
UUID_ORG_B	ORG_B	UUID_L ... UUID_M
...	...	...

FIG. 6B



OBJECT INFORMATION

OBJ. UUID	OBJ. DESC.	ACCESS CONTROL INFO.
UUID_O1	FILE_XYZ	UUID_A
UUID_O2	DB_RECT_ABC	UUID_A, UUID_B
...	...	...

FIG. 6C

FIG. 6A shows user description information including an organization field to specify by UUID the organization(s) to which the user belongs. FIG. 6B shows information specifying the members bound to each organization UUID (*e.g.*, organization A (ORG_A) is comprised of subjects "1" through "L" and organization B (ORG_B) is comprised of subjects "L" through "M").[10] FIG. 6C shows object information (*e.g.*, FILE_XYZ) stored in a private library collection 120 (see below), bound to an object UUID (*e.g.*, UUID_01), and associated with access control objects that are described with an object UUID (*e.g.*, UUID_A) (p. 11, line 7 - p. 12, line 2).[11]

FIG. 7 illustrates an access control system according to the third embodiment and utilizing the above described information. In this embodiment, a user database 400, separate from the administrative database 200, holds user information bound to user UUIDs.

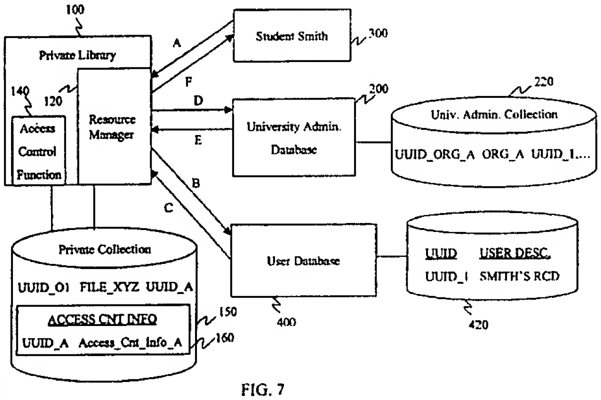


FIG. 7

In this exemplary system, Smith sends a request "A," including Smith's user UUID (UUID_1) and the UUID of the requested file (UUID_01), to the private library access control function 110 for access to FILE_XYZ. Upon receipt of request "A" the access control function 110 resolves Smith's UUID and sends a request "B" to a user database 400 to retrieve subject information about Smith. The user database 400 finds Smith's user information based on the UUID supplied in request "B", and returns "C" a descriptor about the organizations of which Smith is a member (*e.g.*, UUID_ORG_A) (p. 12, line 3 - p. 12, line 10).

[10] This supports the recitation in dependent claim 29 and 32 that "the user information is organization information indicating whether the user is a member of an organization."

[11] This supports the recitation in dependent claim 26 of "wherein the user information includes information relating to an organization of which the user is a member."

The access control function 110 then sends request "D" containing "UUID_ORG A" to the university administrative database 220. The organization information "ORG A" is located in the university administrative collection 220 based on the organization UUID included in request "D". The organization information "ORG A" is then returned in response "E" (p. 12, line 11 - p. 12, line 20).

Based on the returned organization information in "E", access control function 110 determines whether Smith should be granted access to the requested protected object. In this case since Smith is a student of the university, the organization information returned from the university administrative database 200 indicates he is a member of an organization (university students) who by virtue of the agreement are to be provided access to the protected object. Accordingly, access control function 110 returns a response "F" to Smith indicating access to FILE_XYZ is granted (p. 12, lines 21-27).

FIG. 8 illustrates an access control system according to a fourth embodiment of Appellant's invention. This embodiment is similar to the third embodiment, except instead of the access control function 110 resolving UUIDs, the distributed computing system resolves them.

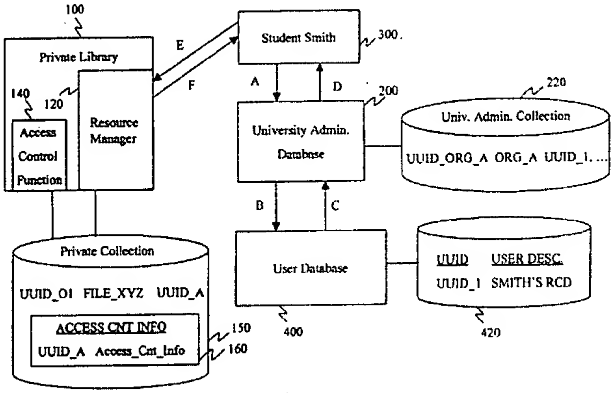


FIG. 8

In this embodiment, when Smith wants to be provided access to a protected object, such as FILE_XYZ in private library collection 120, Smith's computer 300 gathers the information needed by the access control function 110. Specifically, Smith's computer 300 sends a request

"A" to the university administrative database 200 to retrieve organization information for organizations for which Smith is a member. In this example, however, in order to determine those organizations the university administrative database 200 sends to user database 400 a request "B" which includes Smith's UUID (*i.e.*, UUID_1). User database 400 finds Smith's user information (including organization UUIDs describing the organizations in which Smith is a member - UUID_ORG_A) based on Smith's UUID, and returns it in response "C" (p. 13, lines 2-15).

Next, the university administrative database 200 finds the organizations described by UUID_ORG_A, retrieves the organization information needed by the access control function 110, and returns that information to the user's computing system 300 in response "D" (p. 13, lines 15-20).

Once the user's computing system 300 gathers all the information needed by access control function 110 it sends that information (*i.e.*, a request for access to document "x" and an indication that Smith is a student at the university) in a request "E". The access control function 110 then determines if access to the requested object should be granted and returns a yes/no response "F" (p. 13, lines 21-26).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Whether or not claims 1-42 are anticipated by *Garg*.

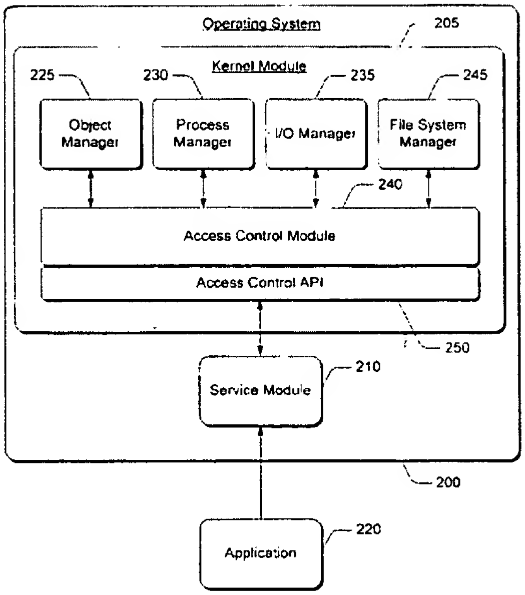
VII. ARGUMENT

I. Current Rejection

As noted above, the Examiner alleges that all of the features of all of the pending claims 1-42 are disclosed by *Garg*. Appellant respectfully disagrees.

II. The Applied Reference - Garg

Garg discloses an access control system (see FIG. 2, reproduced to the right for convenience) that operates within kernel 235 of an operating system 200 of a computer (col. 3, lines 21-26). Each object (*e.g.*, files or folders) stored in the operating system 200 is assigned a GUID that is "not to be re-used by another application" in the operating system 200 (col. 6, line 60 - col. 7, line 6). When applications running in operating system 200 seek to access an object, the applications call service provider module 210, which checks with access control module 240 (col. 13, line 60 - col. 14, line 12) to review an access control list of the object (col. 8, lines 23-28). The access control lists contains USERIDs or GROUPIDs that are allowed access to the object (col. 8, lines 33-38).



Accordingly, while *Garg* does disclose GUIDs identifying particular objects within a system, *Garg* fails to teach or suggest that these GUIDs are in any way unique across different systems. Thus, *Garg's* system still suffers from the same deficiencies as the related art of the instant Application, *i.e.*, that individual administrative domains, such as a university and an affiliated library, must maintain separate redundant access control information. Appellant's specific comments regarding the pending claims follow.

III. Independent Claims 1, 6 and 10

III(a). The Examiner's Position

In both the January 13 and April 20, 2004 *Office Actions*, the Examiner alleges that *Garg* discloses all of the features of independent claims 1, 6 and 10.

Specifically, the Examiner alleges:

(1) that claim 1 and 6's recited "first storage area having an object stored therein," and claim 10's recited "storing [of] an object in the storage system," are shown in FIG. 3A of *Garg*; and

(2) that claim 1 and 6's recited "second storage area having stored therein an object identifier that identifies the object, wherein the object identifier is unique within and outside of the storage system," and claim 10's recited "storing [of] an object identifier in the storage system, wherein the object identifier identifies the object, and the object identifier is unique within and outside of the storage system," are shown in Col. 7, lines 5-6 and Col. 8, lines 10-15.

III(b). Garg Fails to Teach or Suggest All the Features of Claim 1

Appellant respectfully disagrees with the Examiner's position.

As pointed out in the March 14 and June 20, 2004 *Responses* (and as discussed above) *Garg* is directed to an access control system for objects that operates within kernel 235 of a single operating system 200 of a computer (see FIG. 2 and col. 3, lines 6-26). In this regard, Col. 3, lines 6-9 discloses that the *Garg* system (emphasis added):

> **should be implemented by a central module within the operating system** in order to provide a consistent, non-redundant interface.

Further, Col. 6, line 60 - Col. 7, line 6 discloses that (emphasis added):

> Object manager 225 maintains and manages **objects defined within the system**. Objects have properties that are typically used to describe various aspects of the components **of the system**. Many different types of **objects may exist in the system**, and, in one embodiment of the invention, **each object is assigned two unique identifiers known as a Globally Unique Identifier (GUID) to distinguish it from the other objects**. GUIDs are 128 bit numbers and are guaranteed not to be re-used by another application. The first identifier is the Object Type GUID, which identifies the particular **type of object being managed by the object manager**. The second identifier is the Object GUID, which uniquely identifies the **particular object within a group of objects** of the same type.

Thus, it is clear that *Garg* only discloses the provision of an object or object type GUID within **a single storage system** 200, as the only disclosed purpose of the GUIDs of *Garg* is to differentiate the individual objects managed by the object manager 225 within that operating system 200. *Garg* completely fails to teach or suggest that these system-wide GUIDs are in any way unique **outside of the disclosed system** 200.

Thus, regarding claims 1, 6 and 10, Appellant respectfully submits that *Garg* fails to teach or suggest either a storage system, memory or method where an object and an object identifier are stored, where the object identifier identifies the object, and where "the object identifier is unique **within and outside of the storage system**" (emphasis added).

III(c). The Examiner's Further Arguments

The Examiner presents several further arguments in the July 15, 2005 *Final Office Action* and the July 15, 2005 *Advisory Action* in response to the above. Specifically, the Examiner alleges that:

(1) "[t]he GUIDs of *Garg* has [sic] met the claimed limitations of claims 1-16, wherein the claim language states solely the 'object' identifier and not [sic] limited to a 'user'" (*July 15, 2005 O.A.*, pg. 11, lines 3-4); and

(2) "The GUIDs of [*Garg*] are unique that [sic] distinguishes it from the other objects (col. 6, line 65 - col. 7, line 5)" (Attachment to *Advisory Action*); and

(3) "GUIDs are inherently unique identifiers across all computers and networks. GUIDs are 'global unique identifiers' where these identifiers are unique within, outside, or anywhere across all computers and networks in order to [sic] distinct from one object or file to another of another storage or another computer. Else, [sic] the acronym does not accurately define itself. Not only are GUIDs defined as globally unique identifiers but are inherently known to be unique across all computers and networks, therefore [sic] GUIDs of [*Garg*] are unique within and outside of the storage system" (Attachment to *Advisory Action*).

III(d). Appellant's Responses to The Examiner's Further Arguments

Appellant respectfully disagrees with both of the above arguments (1) and (2).

Regarding the Examiner's argument (1), Appellant is not arguing that the recited "object identifier" is directed to a "user" with respect to independent claims 1, 6 and 10 (although such an argument is advanced, when appropriate, with respect to other of the claims discussed herein). Rather, Appellant is arguing that *Garg* fails to teach or suggest any object identifier that "is unique within and outside of the storage system."

Regarding the Examiner's argument (2), Appellants respectfully submit that the GUIDs do not distinguish themselves from "other objects" as the Examiner seems to allege. Rather, the GUIDs differentiate objects from each other.

Regarding the Examiner's argument (3), Appellants respectfully submit that the Examiner has cited no reference that supports her allegation that "GUIDs are inherently unique identifiers across all computers." Nowhere does the sole applied reference, *Garg*, indicate that this is so. In fact, as pointed out above, *Garg* only discloses that the GUIDs distinguish objects from each other **within the system, not external to the system**. Accordingly, the Examiner's position seems merely to be based on conjecture, and is therefore respectfully submitted to be improper.

Appellants also respectfully submit that the Examiner's argument that "the acronym does not accurately define itself" (evidently if "globally" doesn't mean across systems) is also unsupported. In this regard, Appellants believe that the Examiner seems to have concluded that, just because the term "globally" is used, the GUID somehow **must** be "unique across all computers and networks." Appellants respectfully submit that such a conclusion cannot be taken from *Garg*. In fact, rather than adopting the definition of "global" applied by the Examiner, *Garg* actually clearly indicates that the **GUID is unique only across its system**. Thus, the Examiner's alleged definition of "global" - across all computers and networks - is constructed completely from the Examiner's opinion, not the definition disclosed by *Garg*.

In other words, what is relevant in an understanding of Garg is not the broad extremes of what "global" could possibly mean, but **what "global" is described as in Garg's disclosure**. In this regard, "global" only is used to describe the GUID that is unique only within Garg's system, not other systems. Thus, Appellant respectfully submits that there is no teaching or suggestion that "Global" means anything other than **global within system 200**, as discussed above.

IV. Independent Claims 17 and 22

Appellant respectfully submits that *Garg* fails to teach or suggest a method or code for "requesting access for a user to a remote resource, wherein the request includes a subject identifier for use in making an access control decision, and wherein **the subject identifier is unique within and outside of the remote resource and identifies the user**," (emphasis added) as recited in independent claim 17 and 22.

Specifically, Appellants respectfully submit that *Garg* fails to teach or suggest any identifier that "identifies the user" and is "unique within and outside of the remote resource." Rather, the GUIDs cited by the Examiner as allegedly being "unique" **identify objects in the system 200, not users**. The only features in *Garg* that could be read as identifying users are USERIDs or GROUPIDs, which are not disclosed as being "unique within and outside of the storage system" in any way.

The Examiner seeks to overcome these deficiencies by arguing that *Garg* "discloses GroupID which is an [sic] user identifier indicating that the user is a member of along [sic] with other users that has the [sic] similar access rights to the system" (Final *Office Action*, pg. 11, lines 1-3). However, Appellant is not arguing that no user identification is disclosed in *Garg*. Rather, Appellant is arguing that no user identification that is "unique within and outside of the remote resource" is disclosed in *Garg*. Appellants respectfully submit that the user identifier cited above is not indicated to be "unique within and outside of the remote resource."

V. Independent Claim 24

Appellant respectfully submits that *Garg* fails to teach or suggest a method of identifying a user comprising "sending a request for user information from the protecting reference monitor to the resource manager, the request including a subject descriptor for the user, wherein the subject identifier is a Universal Unique Identifier (UUID); receiving, in response to the request, the user information located based on the subject identifier," as recited in independent claim 24.

Specifically, as discussed in detail above, the only identifiers of users in *Garg* are USERIDs and GROUPIDs, neither of which *Garg* indicates to be "unique" in any way. Further, *Garg* fails to disclose the recited requesting and receiving of information on users, as the tabulated USERIDs and/or GROUPIDs are used for access control.

VI. Independent Claim 27

Appellant respectfully submits that *Garg* fails to teach or suggest an information storage management system where "the resource manager receives a user's request for access to the protected object, the request including a globally unique identifier for the user requesting the access, and in response to the user's request the resource manager sends over the communications channel to an external storage management system a request for information about the user, the request including the globally unique identifier," as recited in independent claim 27.

Specifically, *Garg* fails to teach or suggest the provision of a "globally unique identifier" for a "user." As discussed above, the only identifiers of users in *Garg* are USERIDs and GROUPIDs, neither of which *Garg* indicates to be "globally unique" in any way.

Further, *Garg* fails to teach or suggest sending a request to "an external storage management system," or using a received "globally unique identifier" to retrieve information about the user in *Garg*. Rather, as discussed above, *Garg* only utilizes USERIDs and GROUPIDs as a static security list for access control.

VII. Independent Claim 30

Appellant respectfully submits that *Garg* fails to teach or suggest an information storage management system where "the resource manager receives a user's request for access to the protected object, the request including a globally unique identifier for the user requesting the access, and in response to the user's request the resource manager resolves the globally unique identifier to a user identifier recognized by an external storage management system; the resource manager sending to the external storage management system a request for information about the user, the request including the resolved user identifier; and wherein the resource manager upon receiving a response including user information about the user passes the user information to the access control unit; and based on the user information the access control unit determines whether to grant the subject access to the protected object," as recited in independent claim 30.

Specifically, *Garg* fails to teach or suggest the provision of a "globally unique identifier" for a "user," the subsequent use of a received "globally unique identifier" to retrieve information about the "user" in *Garg*, or sending a request to an "external storage medium," for at least the reasons discussed above with respect to independent claim 27.

VIII. Independent Claims 34 and 36

Appellant respectfully submits that *Garg* fails to teach or suggest either a method or code for accessing a protected object comprising "sending a globally unique identifier for a user to a name resolving device, and receiving there from information about the user," and "sending to a storage management system containing an object a request for access to the object, the request including the information about the user," as recited in independent claims 34 and 36.

Specifically, *Garg* fails to teach or suggest the provision of a "globally unique identifier" for a "user." As discussed above, the only identifiers of users in *Garg* are USERIDs and GROUPIDs, neither of which *Garg* indicates to be "globally unique" in any way. Further, as discussed above, there is no teaching or suggestion of any need to send an identifier to a device to receive information about a user in *Garg*, as *Garg* utilizes USERIDs and GROUPIDs as a static security list for access control.

Thus, Appellant respectfully submits that independent claims 1, 6, 10, 17, 22, 24, 27, 30, 34 and 36 are patentable over the applied reference.

Further, Appellant respectfully submits that rejected dependent claims 2-5, 7-9, 11-16, 18-21, 23, 25, 26, 28, 29, 31-33 35, 37 and 38-42 are allowable, *at least* by virtue of their dependency.

VIII. CONCLUSION

In view of the foregoing differences between appealed claims 1-42 and the applied reference, Appellants respectfully submit that appealed claims 1-42 are patentable over the applied reference.

Unless a check is submitted herewith for the fee required under 37 C.F.R. §41.37(a) and 1.17(c), please charge said fee to Deposit Account No. 19-4880.

The USPTO is directed and authorized to charge all required fees, except for the Issue Fee and the Publication Fee, to Deposit Account No. 19-4880. Please also credit any overpayments to said Deposit Account.

Respectfully submitted,

Timothy P. Cremen
Registration No. 50,855

SUGHRUE MION, PLLC
Telephone: (202) 293-7060
Facsimile: (202) 293-7860

WASHINGTON OFFICE
23373
CUSTOMER NUMBER

Date: September 20, 2005

CLAIMS APPENDIX

CLAIMS 1-42 ON APPEAL:

1. (Original) A storage system comprising:

a first storage area having an object stored therein; and

a second storage area having stored therein an object identifier that identifies the object, wherein the object identifier is unique within and outside of the storage system.

2. (Original) The storage system of claim 1, wherein the object identifier is a Universal Unique Identifier (UUID).

3. (Previously Presented) The storage system of claim 1, wherein the first and second storage areas are storage areas within a database.

4. (Original) The storage system of claim 3, wherein the object identifier is a Universal Unique Identifier (UUID).

5. (Original) The storage system of claim 2, wherein the storage system is part of an access control system.

6. (Original) A memory comprising:

a first storage area having an object stored therein; and a second storage area having stored therein an object identifier that identifies the object, wherein the object identifier is unique within and outside of the storage system.

7. (Original) The memory of claim 6, wherein the object identifier is a Universal Unique Identifier (UUID).

8. (Original) The memory of claim 6, wherein the first and second storage areas are storage areas within a database structure.

9. (Original) The storage system of claim 8, wherein the object identifier is a Universal Unique Identifier (UUID).

10. (Original) A method of storing information in a storage system, comprising:

storing an object in the storage system; and

storing an object identifier in the storage system, wherein the object identifier identifies the object, and the object identifier is unique within and outside of the storage system.

11. (Original) The method of claim 10, wherein the object identifier is a Universal Unique Identifier (UUID).

12. (Original) The method of claim 10, wherein the object is stored in a database.

13. (Original) The method of claim 10, wherein the object identifier is stored in a database.

14. (Original) The method of claim 12, wherein the object identifier is a Universal Unique Identifier (UUID).

15. (Original) The method of claim 13, wherein the object identifier is a Universal Unique Identifier (UUID).

16. (Original) The method of claim 10, wherein the storage system is part of an access control system.

17. (Original) An access control method comprising:

requesting access for a user to a remote resource, wherein the request includes a subject identifier for use in making an access control decision, and wherein the subject identifier is unique within and outside of the remote resource and identifies the user.

18. (Original) The access control method of claim 17, wherein the subject identifier is a Universal Unique Identifier (UUID).

19. (Original) The access control method of claim 18, wherein the request further includes a subject descriptor for use in the access control decision.

20. (Original) The access control method of claim 19, wherein the subject descriptor is a UUID for an organizational structure that includes the user.

21. (Original) The access control method of claim 19, wherein the access control decision is made by a resource manager that protects the remote resource, and the request is sent over a communications path considered safe by the protecting resource manager and the user.

22. (Original) A computer-readable medium having computer-executable code stored thereon, comprising:

computer instructions for requesting access for a user to a remote resource, wherein the request includes a subject identifier for use in making an access control decision, and wherein the subject identifier is unique within and outside of the remote resource and identifies the user.

23. (Previously Presented) The access control method of claim 22, wherein the subject identifier is a Universal Unique Identifier (UUID).

24. (Original) A method of identifying a user requesting access to an object, comprising:

establishing a secure communication path between a reference monitor protecting the object and a resource manager having information describing the user, in response to a request by the user to access the object;

sending a request for user information from the protecting reference monitor to the resource manager, the request including a subject descriptor for the user, wherein the subject identifier is a Universal Unique Identifier (UUID);

receiving, in response to the request, the user information located based on the subject identifier.

25. (Original) The method of claim 24, further comprising:

determining, based on the received user information, if the user has permission to access the requested object.

26. (Original) The method of claim 24, wherein the user information includes information relating to an organization of which the user is a member.

27. (Original) An information storage management system, comprising:

a collection of stored objects;

an access control unit for determining if a requestor is authorized to access a protected object stored in the collection;

a resource manager connected to the access control unit and to a communications channel;

wherein the resource manager receives a user's request for access to the protected object, the request including a globally unique identifier for the user requesting the access, and in response to the user's request the resource manager sends over the communications channel to an external storage management system a request for information about the user, the request including the globally unique identifier; and

wherein the resource manager upon receiving a response including user information about the user passes the user information to the access control unit; and based on the user information the access control unit determines whether to grant the subject access to the protected object.

28. (Original) The information storage management system of claim 27, wherein the globally unique identifier is a Universal Unique Identifier (UUID).

29. (Original) The information storage management system of claim 27, wherein the user information is organization information indicating whether the user is a member of an organization.

30. (Previously Presented) An information storage management system, comprising:

a collection of stored objects;

an access control unit for determining if a requestor is authorized to access a protected object stored in the collection;

a resource manager connected to the access control unit and to a communications channel;

wherein the resource manager receives a user's request for access to the protected object, the request including a globally unique identifier for the user requesting the access, and in response to the user's request the resource manager resolves the globally unique identifier to a user identifier recognized by an external storage management system; the resource manager sending to the external storage management system a request for information about the user, the request including the resolved user identifier; and

wherein the resource manager upon receiving a response including user information about the user passes the user information to the access control unit; and based on the user information the access control unit determines whether to grant the subject access to the protected object.

31. (Original) The information storage management system of claim 30, wherein the globally unique identifier is a Universal Unique Identifier (UUID).

32. (Original) The information storage management system of claim 30, wherein the user information is organization information indicating whether the user is a member of an organization.

33. (Original) The information storage management system of claim 30, wherein the resource manager resolves the globally unique identifier by using a name server.

34. (Previously Presented) A method of accessing a protected object, comprising:

sending a globally unique identifier for a user to a name resolving device, and receiving there from information about the user; and sending to a storage management system containing an object a request for access to the object, the request including the information about the user.

35. (Original) The method of claim 34, wherein the globally unique identifier is a Universal Unique Identifier (UUID).

36. (Previously Presented) A computer-readable medium of computer-executable code for accessing a protected object, comprising:

a first set of computer instructions for sending a globally unique identifier for a user to a name resolving device, and receiving there from information about the user; and

a second set of computer instructions for sending to a storage management system containing an object a request for access to the object, the request including the information about the user.

37. (Original) The computer-readable medium of computer-executable code of claim 36, wherein the globally unique identifier is a Universal Unique Identifier (UUID).

38. (New) The storage system of claim 1, wherein the object is a database record describing a user.

39. (New) The memory of claim 6, wherein the object is a database record describing a user.

40. (New) The method of claim 10, wherein the object is a database record describing a user.

41. (New) The access control method of claim 17, wherein the subject identifier identifies a database record describing the user, and the database record is stored on a local resource physically separate from the remote resource.

42. (New) The access control method of claim 22, wherein the subject identifier identifies a database record describing the user, and the database record is stored on a local resource physically separate from the remote resource.

EVIDENCE APPENDIX

This Appendix is Not Applicable to the instant Appeal.

RELATED PROCEEDINGS APPENDIX

This Appendix is Not Applicable to the instant Appeal.